REMARKS

Claims 1-3, 7-12, 15-19, and 21-27 are pending in the instant application. Claims 1-23 presently stand rejected. Claims 1, 7, 12, 15 and 19 are amended herein. Claims 4-6, 13, 14 and 20 are canceled. Claims 24-27 are added. Entry of this amendment and reconsideration of the pending claims are respectfully requested.

Claim Rejections – 35 U.S.C. § 102

The Examiner rejected claims 12-18 under 35 U.S.C. § 101. The Examiner states that the invention is directed to non-statutory result because it is not directed to a "useful, concrete and tangible result." Accordingly, independent claim 12 has been amended to overcome the rejection. The Applicants respectfully request that the instant rejection of claim 12 and its corresponding dependent claims be withdrawn.

Claim Rejections – 35 U.S.C. § 102

Claims 1-23 stand rejected under 35 U.S.C. § 102(a) as being anticipated by "Terra: A Virtual Machine-Based Platform for Trusted Computing, " by Garfinkel et al. ("*Garfinkel*"). Applicants respectfully traverse the rejections.

A claim is anticipated only if each and every element of the claim is found in a single reference. M.P.E.P § 2131 (citing *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628 (Fed. Cir. 1987)). "The identical invention must be shown in as complete detail as is contained in the claim." M.P.E.P. § 2131 (citing *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226 (Fed. Cir. 1989)).

Amended independent claim 1 now recites, in pertinent part, "**using a trusted hardware device** shared between the first and the second VM **to compute a compound hash value** based on a combination of the first VM platform configuration including [a] first hash value and the second VM platform configuration including [a] second hash value," and "storing the compound hash value in the trusted hardware device." Applicants respectfully submit that *Garfinkel* fails to disclose at least the above limitation.

The Examiner cites the right column of p. 196 of *Garfinkel* as corresponding to Applicants' previous claim 14. In the cited sections of *Garfinkel*, however, Applicants have not found any reference to a computation or determination of a compound hash value based on a first and a second virtual hash value. The referenced section of *Garfinkel* discusses establishing trust by using two certificate chains to show that a VM with a particular hash is running and that the hash represents a particular version of a particular software program (see second full paragraph, p. 196). *Garfinkel* discloses verifying one or more hash numbers in the attestation process, however, *Garfinkel* does not disclose "determining a compound hash value..." and "storing the compound hash value in a trusted hardware device shared between the first and second VM using the VMM multiplexer." See also page 14 of the Applicants' specification for the security benefits associated with the use of a compound hash value.

Consequently, *Garfinkel* fails to disclose each and every element of claim 1, as required under M.P.E.P. § 2131. Independent claims 12 and 19 include similar novel elements as independent claim 1. Accordingly, Applicants request that the instant §102 rejections of claims 1, 12 and 19 be withdrawn.

The dependent claims are novel over the prior art of record for at least the same reasons as discussed above in connection with their respective independent claims, in addition to adding further limitations of their own. Accordingly, Applicants respectfully request that the instant § 102 rejections of the dependent claims be withdrawn.

New Claims

New independent claim 24 recites:

24. A method, comprising:

loading **an untrusted** virtual machine monitor (VMM) to support a plurality of virtual machines in a computer system, the VMM including a VMM multiplexer;

loading a first and a second virtual machine (VM) supported by the VMM;

sharing a trusted hardware device between the first VM and the second VM using the VMM multiplexer.

Independent claim 24 is not anticipated by Garfinkel for at least the reasons stated below. Applicants' claim 24 includes loading an **untrusted** virtual machine monitor to support a plurality of virtual machines in a computer system. The VMM in Garfinkel is referred to a Trusted Virtual Machine Monitor (TVMM) because it acts as a trusted party to authenticate the software running in a VM to remote parties (see Garfinkel, p. 194 under "Terra Architecture"). In contrast, claim 24 includes a VMM that can remain **untrusted** because the **trusted logic remains with TPM 106**. In embodiments of the Applicants' invention, it is not necessary for the VMM to be trusted or perform the security functions that are performed by the TVMM in Garfinkel because of the security functions performed by the TPM. See p. 10, line 1-2 and also Figs. 4A-4B and Fig. 5 of Applicants' specification. New dependent claims 25-27 have also been added. Applicants respectfully request consideration of the claims.

CONCLUSION

In view of the foregoing amendments and remarks, Applicants believe the applicable rejections have been overcome and all claims remaining in the application are presently in condition for allowance. Accordingly, favorable consideration and a Notice of Allowance are earnestly solicited. The Examiner is invited to telephone the undersigned representative at (206) 292-8600 if the Examiner believes that an interview might be useful for any reason.

CHARGE DEPOSIT ACCOUNT

It is not believed that extensions of time are required beyond those that may otherwise be provided for in documents accompanying this paper. However, if additional extensions of time are necessary to prevent abandonment of this application, then such extensions of time are hereby petitioned under 37 C.F.R. § 1.136(a). Any fees required therefore are hereby authorized to be charged to Deposit Account No. 02-2666. Please credit any overpayment to the same deposit account.

Respectfully submitted,
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP

Date: February 28, 2007

Linda Zachariah
Reg. No. 48,057
Phone: (206) 292-8600